(12) UK Patent Application (19) GB (11) 2 397 731 (13) A

(43) Date of A Publication 28.07.2004

(21) Application No: 0301476.8

(22) Date of Filing: 22.01.2003

(71) Applicant(s):
eBizz Consulting Limited
(Incorporated in the United Kingdom)
41 Tabernacle Street, LONDON,
EC2A 4AA, United Kingdom

(72) Inventor(s):
Patrick Matthew Carroll
Michael James Skells

(74) Agent and/or Address for Service:
Reddie & Grose
16 Theobalds Road, LONDON, WC1X 8PL,
United Kingdom

(51) INT CL^7:
H04L 9/32 , G06F 1/00 , H04L 29/06 , H04Q 7/38

(52) UK CL (Edition W):
H4P PDCSA
H4L LRCMA

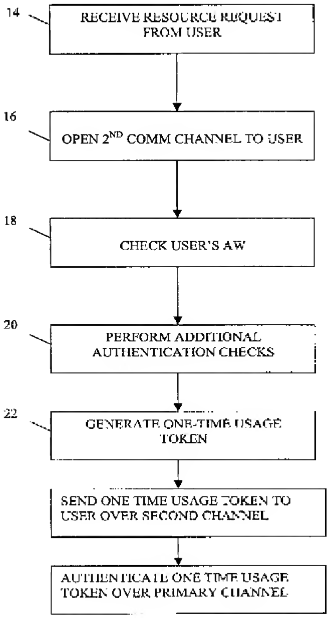
(56) Documents Cited:
GB 2377523 A
WO 2002/019593 A2
WO 2001/044940 A1
EP 1107089 A1
WO 2001/099378 A1
WO 2001/015381 A1

(58) Field of Search:
UK CL (Edition V) H4L, H4P
INT CL^7 G06F, H04B, H04L, H04M, H04Q
Other: Online: WPI, EPODOC, PAJ

(54) Abstract Title: **Authenticating a user access request to a secure service over a primary communication channel using data sent over a secondary communication channel**

(57) A method and apparatus are provided for authenticating a user access request 14 to a secure service over a primary communication channel. At least one secondary substantial real-time communication channel is also opened 16. An authentication process is then performed, with at least part of this process being performed over the secondary channel. Access to the secure service is authorised over the primary channel in dependence on the result of the authentication.

The secondary channel may be a telecommunications channel and may be used to deliver a users PIN. Furthermore the authorizing may involve generating a one time usage token 22 which may only be usable only for a predetermined time period, and the usage token may be delivered to the user via the secondary channel.


14
RECEIVE RESOURCE REQUEST FROM USER
16
OPEN 2ND COMM CHANNEL TO USER
18
CHECK USER'S AW
20
PERFORM ADDITIONAL AUTHENTICATION CHECKS
22
GENERATE ONE-TIME USAGE TOKEN
SEND ONE TIME USAGE TOKEN TO USER OVER SECOND CHANNEL
AUTHENTICATE ONE TIME USAGE TOKEN OVER PRIMARY CHANNEL

GB 2 397 731 A

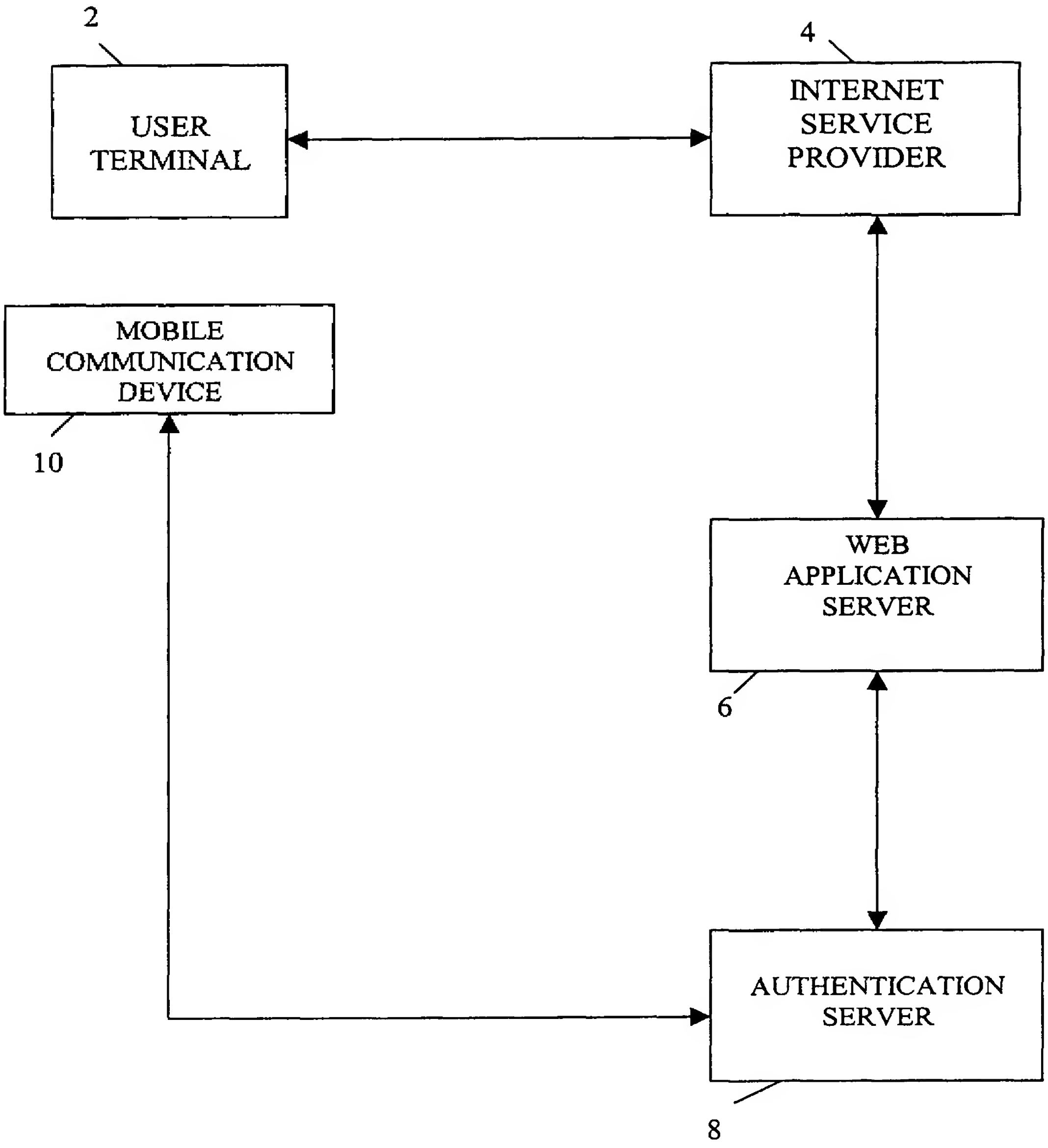

2
USER TERMINAL
4
INTERNET SERVICE PROVIDER
MOBILE COMMUNICATION DEVICE
10
WEB APPLICATION SERVER
6
AUTHENTICATION SERVER
8

Figure 1

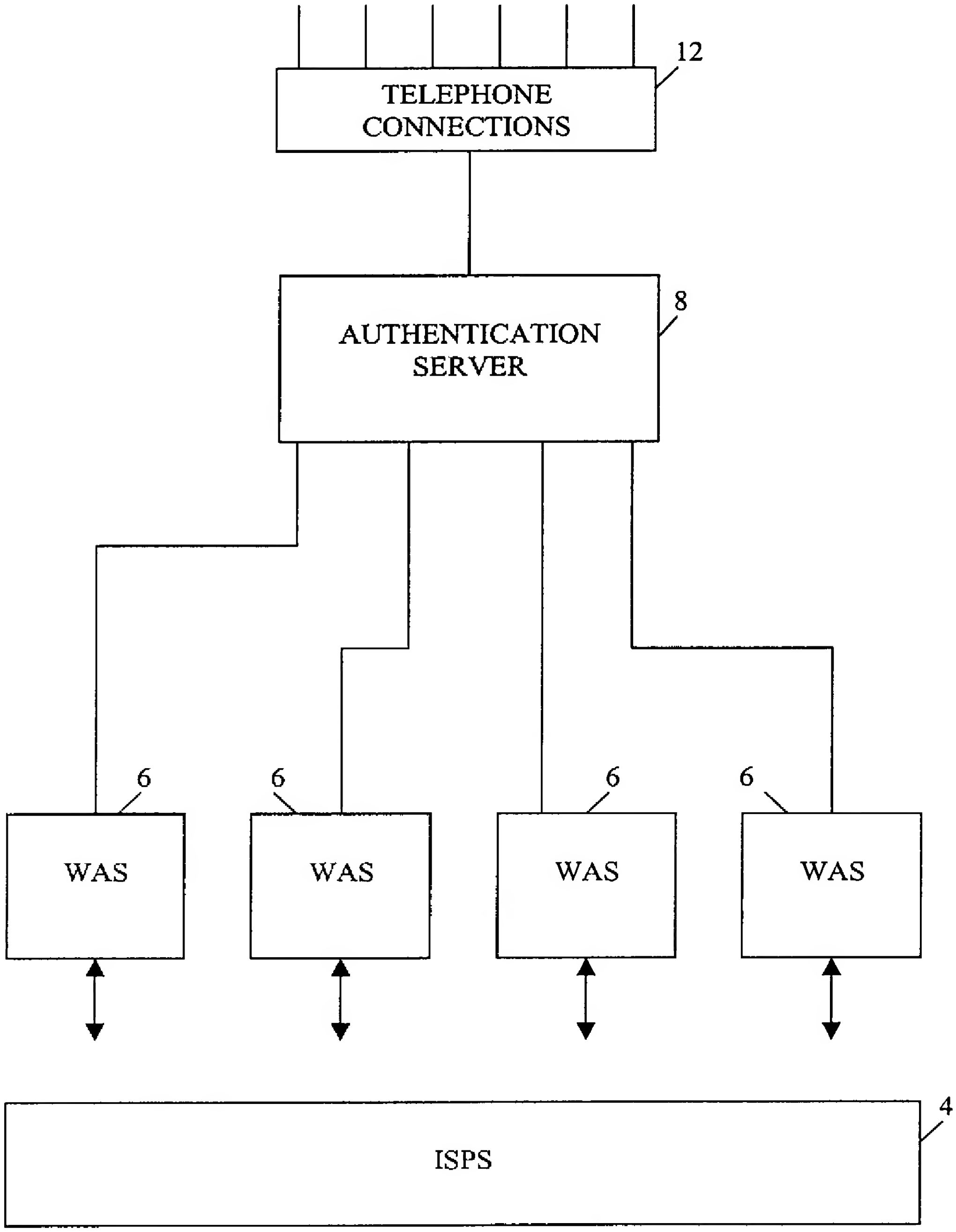
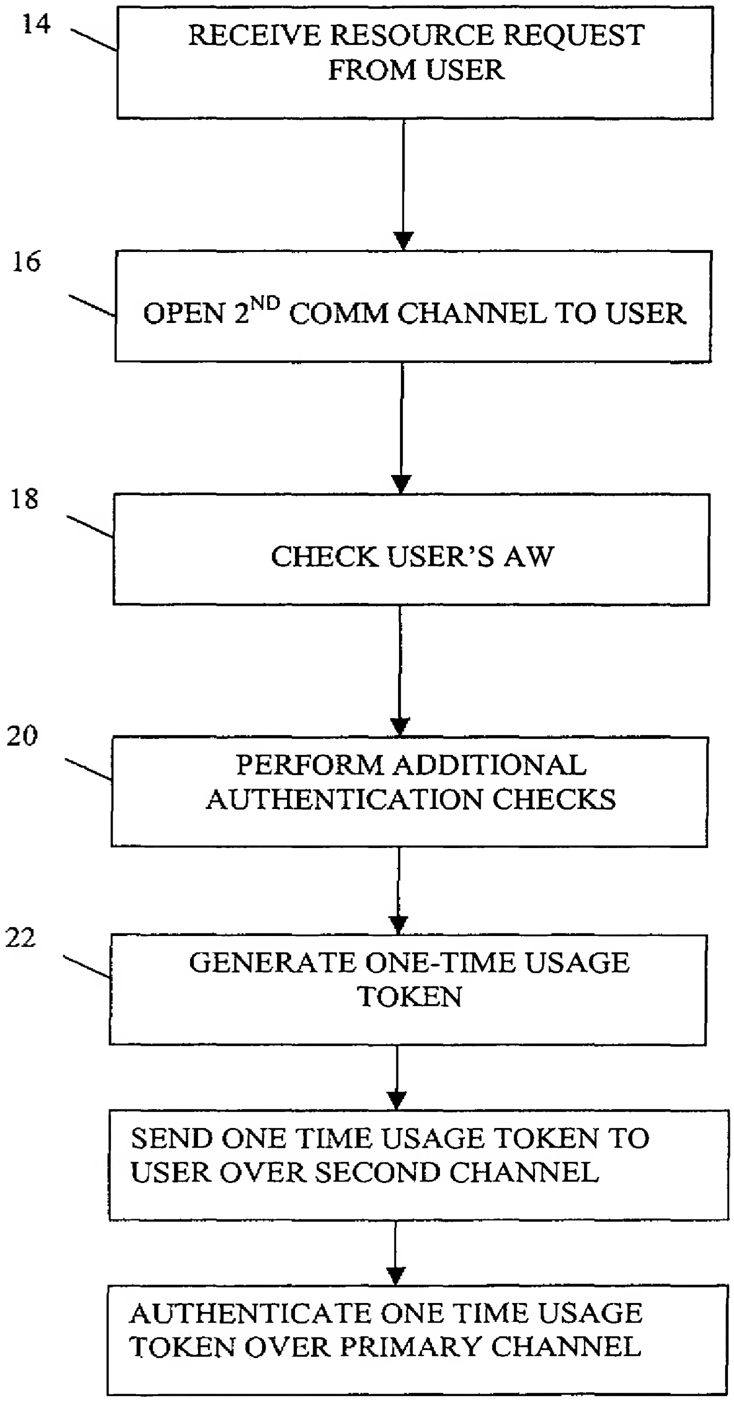

12
TELEPHONE CONNECTIONS
8
AUTHENTICATION SERVER
6
6
6
6
WAS
WAS
WAS
WAS
4
ISPS

Figure 2


14
RECEIVE RESOURCE REQUEST FROM USER
16
OPEN 2ND COMM CHANNEL TO USER
18
CHECK USER'S AW
20
PERFORM ADDITIONAL AUTHENTICATION CHECKS
22
GENERATE ONE-TIME USAGE TOKEN
SEND ONE TIME USAGE TOKEN TO USER OVER SECOND CHANNEL
AUTHENTICATE ONE TIME USAGE TOKEN OVER PRIMARY CHANNEL

AUTHENTICATION SYSTEM

This invention relates to an authentication system of the type which provides an authorisation to gain access to a secured computer service. A computer service includes a specific computer application or resource, and computer authorisation for specific transactions e.g. fund transfers.

Two factor authentication systems are used widely. Usually they require the use of a hardware token device which is carried by a user in combination with a Personal Identification Number (PIN). The hardware token device in combination with the PIN is able to provide a usage token to gain access to a secured service. Typically this is done by a synchronisation process with a server protecting the service. The usage token may be a one time usage token. It may have an expiry time, it may also provide access for a predetermined amount of access time e.g. 2 hours.

If a user requires access to more than one secured service then he will usually have to carry with him a hardware token device for each service. Because of this, recent developments have used the short messaging service provided by mobile phones to transmit a usage token to the user. This is dependent on the user first having correctly entered his PIN into the secured service, usually over the Internet, and possibly also to have answered some personal authentication questions in addition to entry of the PIN. Similarly, some products have also started to use e-mail as the delivery mechanism for the token. This is similar in principal to SMS.

Problems with hardware token devices arise because they can easily be mislaid or stolen. They typically also have a limited life and have to be replaced periodically. The activation process when they are issued is complex and requires co-ordination between system set-up, physical delivery of the tokens, and password activation management. They are generally expensive to produce and manage and usually have structures which make them unattractive to many potential users.

Mobile SMS or e-mail options also have problems specific to them. They are not generally regarded as secure delivery services and can easily be hacked into. Also, neither service can guarantee delivery within a particular short time span. They currently work in the outbound direction from a server to a recipient. Therefore, they may incur a cost on the service provider, which would not otherwise be there. Also, this type of messaging does not enable any PIN security to be placed on messages, which include the usage tokens, thereby reducing the security of the system.

We have appreciated that the need for a user to carry a hardware device or to rely on SMS or e-mail delivery of messages can be eliminated.

Accordingly, preferred embodiments of the invention provide an authentication system which uses at least one secondary communication channel at least partially in an authentication process to generate a usage token for a secured service so that access can be made to the secured service over a primary communication channel.

The secondary channel may be a pre-existing channel or a new channel. When reference is made to opening a channel, this may mean opening a new channel or the use of a pre-existing channel. The pre-existing channel may be in place due to the method of operation of the service provider of the secondary channel. For example, it may be there because there is a mobile phone protocol for management channel information, this is the channel used to advise users that there is voicemail waiting, advises users of the local operator name, etc. or it may be established by some software present, e.g. in the operating system, the SIM card, or other means on the device, or for any other reason.

Preferably the secondary channel is used to communicate the one time usage token to the user.

Preferably the secondary channel is a telecommunication channel.

Preferably the secondary channel is used for delivery of a user's PIN to the service.

Preferably the service and the user both communicate with a further server via the primary and secondary channels which further server performs at least part of the authentication process.

Preferably the further server communicates with the user via the secondary channel.

Preferably the further server can communication with the user via the primary channel.

Preferably the further server is able to perform authentications for a plurality of secured services.

Preferably the further server is able to perform authentications for a plurality of different servers.

The primary and secondary channels may be formed over physically separate links e.g. Internet dial-up and mobile telephone. Alternatively they may be provided via the same physical connection (telecommunications cable) but be effectively separate by the use of different communications protocols, or connections.

The invention is defined with more precision in the appended claims to which reference should now be made.

A preferred embodiment of the invention will now be described in detail by way of example with reference to the accompanying drawings in which:

Figure 1 shows a block diagram of a system embodying the invention;

Figure 2 shows a block diagram of an authentication server embodying the invention; and

Figure 3 is a flow chart showing how the authentication process operates.

Figure 1 shows a user terminal 2. This will typically be a personal computer. In this example it is a personal computer at a remote location. Using a conventional telephone connection e.g. DSL, leased line. Satellite, radio etc., the user uses the user terminal to connect to a communications network e.g. an Internet service provider (ISP) 4 using well-known techniques. Using the Internet service provider, the user is then able to request access to a particular service stored on a web application server. This is a secured service and requires an authentication process to be completed before the user can access it.

The web application server 6 is connected to an authentication server 8 which it uses to perform authentication.

The user requests a service in the secured application via the ISP. The request gets as far as the web application server which informs the authentication server 8 that an authentication for a particular service on the web application server 6 is required, and it is ready to start an authentication process.

A further communication channel is opened to the user. Typically this is to a mobile communication device 10 such as a mobile telephone or PDA. The device could also be a standard telephone connected via a landline to the authentication server 8. The connection between the authentication server 8 and the communication device 10 can be instigated in a number of different ways. One option is for the authentication server to notify the user terminal 2 via the web application server and the ISP 4 that it is now ready to receive a call from the communication device 10 which will open the second communication channel. The user then calls the authentication server on his mobile communication device 10 using a number he either knows or is advised of by the authentication server 8 via the web application server and the ISP 4. The second communication channel is then opened.

Alternatively, the user may be asked for a number from a known set of numbers, or a new number which should be called in order to open up the second communication channel to the mobile communication device 10. This number is then dialled by the authentication server and the call answered by the user, thereby opening the channel.

Once both channels are open, the authentication process can continue.

The authentication server then uses the communication channels via the web application server and the Internet service provider and via the mobile communication device 10 to ask the user a question or series of questions to determine whether or not a one time usage token to enable access to the secure service should be issued.

The questions asked of the user will typically include a request for either his PIN or a selected subset of his PIN. It may also include additional questions e.g. date of birth of user, mothers maiden name etc. These types of questions are well-known in authentication systems for assuring that the person who is requesting access is who he claims to be. All of the above may request the full answer or some subset of it.

The embodiment of the invention shown in figure 1 uses both of the communication channels to perform the authentication although it could take place only in the second communication channel. The second communication channel is the more secure channel. Preferably most of the users responses to the questions will be provided via the second communication channel as this means the service is protected by two separate communication protocols, potentially over two separate bearers. The user may be requested to put forward his PIN which he may enter via the keypad of a mobile phone which generates touch tone signals or he may speak into the mobile and the PIN is recognised by suitable voice recognition. These are recognised by the authentication server 8 and the PIN can be checked against that stored for a particular user.

To take full advantage of the two channels available for authentication, it is possible for questions to be asked via one channel and for answers to be given via the other. As the second channel is opened via the mobile communication device 10 it is a separate channel, and it is preferable that the answers be provided on this channel. Questions can be asked either through the user terminal via the first communication channel or directly to the mobile communication device 10. Question generation is automatic and is stored in the software of the authentication server.

The authentication server can communicate with the mobile communication device 10 using the channel as a voice channel, in which case it will require some means to generate a voice signal.

Thus, it can be seen, that the secondary channel provided to the mobile communication device 10 provides a two-way communication link which can be used in the authentication process.

Once the authentication server 8 is satisfied that the user is who he claims to be, the authentication server can proceed to enable access to the resource. This can be done in a number of ways. A usage token can be provided via the voice channel to the mobile communication device 10 where the user hears it and types it into the user terminal 2. It is then provided via the ISP 4 to the web application server 6 where it is verified by the web additional server. If this verification succeeds it enables access to be made to the selected service by the user who is then able to use the user terminal 2 to use that service.

In an alternative embodiment, the authentication server 8 can provide the authentication to proceed directly to the web application server 6 via its link to that server. The user is then advised that access is possible via the ISP 4 and his terminal 2 and can then start to use the service, or the access may proceed automatically.

The system can be adapted to require different users to go through different authentication processes. These can vary the authentication process and questions asked each time a user tries to make access to a resource. It can also vary the process according to the delivery medium being used for the usage token or any other reason.

The use of the direct telephone link to the mobile communication device 10 means that immediate delivery of tokens to a user can be made. In addition the fact that the channel to the communication device 10 is two way means that a much more thorough authentication process can take place via this more secure link than could take place via the ISP link to the user.

The fact that a voice channel is used means that immediate delivery of tokens is possible thus overcoming the problems normally associated with SMS messaging and e-mail delivery of tokens. However future SMS and email services may provide effective immediate delivery services.

Preferably the authentication server 8 is a third party server which provides an authentication service to a plurality of different web application servers. Such an arrangement is shown in figure 2. In the Figure it can be seen that the authentication server 8 is coupled to a plurality of web application servers 6. Each of these in turn may have a plurality of different resources which users may wish to connect to via the Internet. Thus, the web application servers 6 are all capable of communicating with one or more Internet service providers 4 via Internet connections.

Preferably the web application server is configured to provide services even in the event of some failure by using known techniques such as clustering, dual redundant servers, etc.

The authentication server 8 has a plurality of telephone connections 12 available to it, which it can use to dial individual users who might request via the Internet to have access to resources provided on one of the web application servers 6. They may also be configured to receive calls from users

Figure 3 shows a basic flow diagram of one possible operation of the authentication server 8. At 14, a resource request is received from a user. At 16 a second communication channel (the voice channel) is opened to a user. At 18 a user's PIN is checked. This is done by asking for the whole PIN or for a particular subset of it. After this, at 20 other additional authentication checks are performed by prompting the user for responses to various questions. This authentication process as discussed before preferably takes place via the voice channel or via a combination of the voice channel and the Internet connection. If all the checks are satisfactory then at 22 the necessary usage token can be generated and provided to the user or directly to the requested resource.

Sending requests for a PIN and receiving a response over the voice line to the mobile communication device 10 severely restricts the possibility of hacking into the system.

The functions of logging on via the user identifying himself requesting a resource over the Internet and PIN identification are split between two communication channels, the chance of a hacker obtaining all the data required to access the resource are again severely restricted since flowing conversations would have to be intercepted as well as the Internet connection having to be accessed.

One way in which this authentication service can be made attractive to potential customers arises from the arrangement whereby a user is instructed to ring in to the authentication server 8. If a premium price option is in use then this enables the provider of the resource to increase the cost of calls made to the authentication server 8. Thus, each time the authentication request is made additional revenue can be contributed to the owner of the requested resource. The amount could be significant for a much requested resource. Thus by the simple step of charging an increased call charge to a user for every authentication request, additional profits can be generated for this resource provider without any apparent increase in the standard charge of resource access made to the user.

In this case where the authentication server is providing authentication to a plurality of different services or to different servers, all owned by different parties, the authentication server is preferably owned by a single party which provides an authentication service to provide access to the other services. Thus there are further options for raising revenue here by a third party which may take percentage of call charges made in authentication requests by users.

Various modifications to the embodiment described are possible. The access from user terminal need not necessarily be via a network. It may be a more secure dial up connection. It may be to a particular application provided on a stand alone computer. In such a case the communication channel to the service is internal to the computer. However the security of the authentication process is still improved by using the additional channel to the mobile communication device 10 in the authentication process.

The two channels may be via the same network. They may be represented as different windows on the same computer display. The user may be a computer application requesting access to a secured service. In which case the secondary channel may be connected to the computer application or some other third party.

Token generation and delivery may take place prior to access being requested to the secured service.

Access may be for a period of time and may subsequently be revoked at the time of expiration or in response to some other event, e.g. break-in detection.

The system can be set up to enable a user to enter an emergency PIN. This would notify the service of an emergency. It would then appear to the user to operate as normal, but in fact the apparent operation would not take place. This would be useful if a user was being threatened by a third party to provide access to the secured service.

The secured service may include a resource, an application, some part of an application, or a transaction. In the latter case a new authentication will preferably be required for each access.

A simplified authentication process may involve the authentication system recognising a call from a known user's mobile communication device and providing a usage token or other authority to proceed directly to the service without answering the call, thereby saving costs.

The authentication process could all take place in the server on which the requested service resides.

CLAIMS

1. A method for authenticating a user access request to a secured service over a primary communication channel comprising the steps of:

opening at least one secondary substantially real time communication channel to the user;

performing at least part of an authentication process over the secondary channel; and

authorizing access to be made to the secure service over the primary channel.

2. A method according to claim1 in which the authorizing step includes the step of generating a usage token.

3. A method according to claim 2 in which the usage token comprises a one time usage token.

4. A method according to claim 2 or 3 in which the usage token is usable only for a predetermined period of time.

5. A method according to any preceding claim in which only the secondary channel is used in the authentication process to cause the authorization to be generated.

6. A method according to claim 2, 3 or 4 in which the usage token is delivered to the user via the secondary channel.

7. A method according to any preceding claim in which the secondary channel is a telecommunications channel.

8. A method according to any preceding claim in which the secondary channel is used to deliver a user's PIN.

9. A method according to any preceding claim in which the method is performed by an authentication server coupled to the primary and secondary channels.

10. An authentication system to provide access to a secured service over a primary communication channel over which access requests are received, a secondary substantially real time communication channel, means for generating an authorization for the secured service, and means for performing at least part of an authentication over the secondary communication channel.

11. A system according to claim 7 in which access to the service is provided over the primary channel and only the secondary channel is used in the authentication process to cause the authorization to be generated.

12. A system according to claim 7 or 8 in which the usage token is delivered to the user via the secondary channel.

13. A system according to claims 7, 8 or 9 in which the secondary channel is a telecommunications channel.

14. A system according to any of claims 7 to 10 in which the secondary channel is used to deliver a user's PIN.

15. A system according to any of claims 7 to 11 comprising an authentication server coupled to the primary and secondary channels and also coupled to a separate server on which the secured service is located.

16. A system according to claim 12 in which the authentication server is coupled to a plurality of servers on which secured services are located.

Application No:	GB 0301476.8	**Examiner:**	Adam Tucker
Claims searched:	1-16	**Date of search:**	9 May 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance	
X, Y	X: 1-16 Y: 1-16	WO 01/99378 A1	(ICL Invia OYJ) See whole document
X, Y	X: 1-16 Y: 1-16	WO 01/044940 A1	(Authentify Inc.) See whole document
X, Y	X: 1-16 Y: 1-16	WO 01/15381 A1	(Danal Co.) See whole document
Y	1-16	GB 2377523 A	(Netdesigns Limited) See whole document
Y	1-16	EP 1107089 A1	(Connectotel) See whole document
Y	1-16	WO 02/19593 A2	(Ericsson) See whole document

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category	P	Document published on or after the declared priority date but before the filing date of this invention
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{V}:

H4L, H4P

Worldwide search of patent documents classified in the following areas of the IPC^{7}:

G06F, H04B, H04L, H04M, H04Q

The following online and other databases have been used in the preparation of this search report:

WPI, EPODOC, PAJ